GRAPHICAL PASSWORD AUTHENTICATION USING PASS POINT SCHEME

A Mini Project Report

submitted by

SUSHNA(MES20MCA-2055)

to

the APJ Abdul Kalam Technological University
in partial fulfillment of the requirements for the award of the Degree

of

Master of Computer Applications

Department of Computer Applications

MES College of Engineering
Kuttippuram, Malappuram - 679 582

February 2022

DECLARATION

I undersigned hereby declare that the project report **GRAPHICAL PASSWORD AUTHENTICATION USING PASS POINT SCHEME**, submitted for partial fulfillment of the requirements for the award of degree of Master of Computer Applications of the APJ Abdul Kalam Technological University, Kerala, is a bonafide work done by me under supervision of Mr.Nowshad C V, Assistant Professor, Department of Computer Applications. This submission represents my ideas in my own words and where ideas or words of others have been included, I have adequately and accurately cited and referenced the original sources. I also declare that I have adhered to ethics of academic honesty and integrity and have not misrepresented or fabricated any data or idea or fact or source in my submission. I understand that any violation of the above will be a cause for disciplinary action by the institute and/or the University and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been obtained. This report has not been previously formed the basis for the award of any degree, diploma or similar title of any other University.

Place:

SUSHNA(MES20MCA-2055)

Date:

DEPARTMENT OF COMPUTER APPLICATIONS
MES COLLEGE OF ENGINEERING, KUTTIPPURAM

CERTIFICATE

This is to certify that the report entitled **GRAPHICAL PASSWORD AUTHENTICATION USING PASS POINT SCHEME** is a bonafide record of the Mini Project work carried out by **SUSHNA(MES20MCA-2055)** submitted to the APJ Abdul Kalam Technological University, in partial fulfillment of the requirements for the award of the Master of Computer Applications, under my guidance and supervision. This report in any form has not been submitted to any other University or Institution for any purpose.

Internal Supervisor(s) External Supervisor(s)

Head Of The Department

Acknowledgements

At the very outset I would like to thank the almighty's mercy towards me over the years... I wish to express my sincere thanks to my project guide Ms.Priya J.D Assistant professor, Dept. of Master of Computer Applications who guided me for the successful completeness of this project. I also thank her for valuable suggestions, guidance, constant encouragement, boundless corporation, constructive comments and motivation extended to me for completion of this project work.

I would express my sincere thanks to my internal guide Mr.Nowshad C V,Assistant Professor for their immense guidance to complete the project successfully.

I would like to express my sincere thanks to all the faculty members of Master of Computer Applications department for their support and valuable suggestion for doing the project work.

Last but not least my graceful thanks to my parents, friends and also the persons who supported me directly and indirectly during the project.

SUSHNA(MES20MCA-2055)

Abstract

Graphical passwords are an alternative to alphanumeric passwords in which users click on images to authenticate themselves rather than type alphanumeric strings. We have developed one such system, called Pass Points, and evaluated it with human users. The results of the evaluation were promising with respect to memorability of the graphical password.We develop a model to identify the most likely regions for users to click in order to create graphical passwords in the Pass Points system. A Pass Points password is a sequence of points, chosen by a user in an image that is displayed on the screen. Our model predicts probabilities of likely click points; this enables us to predict the tolerance of a click point in a graphical password for a given image.

At the authentication time, we are checking whether the pass point we clicked is correct or not.

Keywords: Graphical password,Pass point,Authentication.

Contents

List of Figures

Chapter 1

Introduction

1.1 Background

Authentication is the first line of defence against compromising confidentiality and integrity. Alphanumerical usernames and passwords are the most common method of computer authentication.This method has many drawbacks. Usually people use passwords that can be easily guessed, so that it does not becomes hard to remember

Hence to encounter this problem, researches have developed graphical password authentication methods that use pictures as passwords. Graphical passwords are an alternative to text-based passwords where user is asked to recall an image or parts of an image instead of a word.We are further discussing new and more secure graphical password system called pass points.

In pass points system users can create many points click sequence on a background image. The graphical password is new technique which is more secure than text-based passwords . In graphical passwords, sequence of clicks is generated to derive the password. The click events are performed on same image or different image. Or users can also select sequence of images. Users can submit image then he/she can click on the image to create a password then the system pixel tolerance calculates each pixel around. And then while authenticating user needs to click within the tolerances in the correct sequences.

1.1.1 Motivation

The main motivation for graphical passwords is the hypothesis that people are better at remembering images than artificial words. Visual objects seem to offer a much larger set of usable passwords. For example we can recognize the people we know from thousands of faces; this fact was used to implement an authentication system . As another example, a user could choose a sequence of points in an image as a password; this leads to a vast number of possibilities,if the image is large and complex, and if it has good resolution. This is the basis for the graphical passwords . An excellent survey of the numerous graphical password schemes that have been developed such as; Recognition based systems,Pure recall based systems,Cued recall based systems.

1.2 Objective

The main objectives are:

- The system is user-friendly and has simple interface.
- Provides strong security against bot attacks or hackers.
- Protects systems vulnerable to attacks.
- This system can be used by the multiple peoples to get the counselling sessions online.

1.3 Report Organization

The system contain two section : Registration part and Main part.

Clicking points for password is done at registration part and checking whether password clicked is correct or not is done at main part.

Chapter 2

Literature Survey

Suvarana Pansambal (Shirke) and et al [12], summarizes the concept of graphical password system. in which there is an image. In the next stage user select number of click points on image. In the registration user gets to generated click points of the image. While logging in user has to click point for authentication.

Sruthi P V had been done work on graphical password authentication. In registration phase user enters all details and selects point on images. The system will send a random dynamic string/word to the user by email. Then in the next page, an images set, each with different meaningful word will be displayed. Now, user will click on the image with the same string/ word that he received by email. Tara H R and et a primarily focus on click-based graphical passwords. During password creation, user has to select the images along with its click points. At the time of authentication, user has to select the correct click point on each of the images. During authentication, system decides the first image to be displayed. User has to enter click point on the image as images are displayed one after the other on the screen. Click point on each image decides the next image.

Ansari Ahmed and et al designed click point based technique. During the registration phase user has to enter all details. Then user has select images on the client machine storage or at the server side. To protect the integrity of the system, they had introduced PASSPOINTS and password fields. When the user is asked to enter the points for authentication he may enter n number of points on the images, in any sequence. But during login process the user must enter the points in same sequence as clicked in the registration process

Atish Nayak and Rajesh Bansode , targets on the integral evaluation of the Persuasive

Pass Points graphical password system which includes usability and security evaluation on three different levels. This paper used persuasive to impact user choice is used in clickbased graphical passwords for motivating users to select more random, and hence more difficult to guess, clickpoints.

Nikhil Bomanwar and Neha Singh, this paper briefly describes the different Graphical Authentication Schemes. Pass points, passwords consist of a sequence of five click points on a given image PassPoint consists of password creation, wherein the user has to select the images, sequence of the images and a click point for each image. This paper also brings to notice the Persuasive Technology which guides and encourages users to select robust passwords, but not force system generated passwords.

Uma D. Yadav and Prakash S. Mohod , focuses on adding more features in existing graphical password schemes. The improvements are brought about by adding the concept of modules wherein the first module deals with setting the seed value or unique and the latter deals with offering tolerance. In short this paper comprises the improvements in the existing system.

Chapter 3

Methodology

3.1 Introduction

In pass points system users can create many points click sequence on a background image. The graphical password is new technique which is more secure than text-based passwords . In graphical passwords, sequence of clicks is generated to derive the password. The click events are performed on same image or different image. Or users can also select sequence of images. Users can submit image then he/she can click on the image to create a password then the system pixel tolerance calculates each pixel around. And then while authenticating user needs to click within the tolerances in the correct sequences.

The system contain two section : Registration and Main part. Clicking points for password is done at registration part and checking whether password clicked is correct or not is done at main part.

Algorithm used is Tolerance calculation algorithm , in which tolerance is calculated for the click points. The algorithm helps to find the nearest place where we clicked and will form a square , inside it any where we can click for our password.

There are four points we have to click and at the fourth click a message box appear as, ”Successfully saved ”.if we click ’ok’ button of message box, a reference image of click points will appear.

At the authentication,we have to click four points and then check whether the points are same or not.A message box will appear as,”pass point correct” if it is matched and ”pass point error” if they are not matched.

The system is more applicable in Digital wallets and Crypto currency because it is hard method.

3.2 Developing Environment

HARDWARE SPECIFICATION:

1. Processor: i3 Based Computer or higher
2. Memory: 1 GB RAM
3. Hard Drive: 50 GB
4. Monitor
5. Internet Connection

SOFTWARE SPECIFICATION:

1. Language :Python
2. Front end : Python
3. Back end : Python
4. Operating system : windows 7 and above
5. IDE : PyCham

3.3 Agile Methodology

The Agile methodology is a way to manage a project by breaking it up into several phases.It involves constant collaboration with stakeholder and continues improvement at every stage.Once the work begins,teams cycle through a process of planning,executing and evaluating.Continuous collaboration is vital,both with team members and project stakeholders. The project is divided into three modules:

Sprint 1:Registration and Algorithm implementation

i)Defining Click points
ii)Algorithm Implementation
iii)Save to Dataset

Sprint 2:Authentication

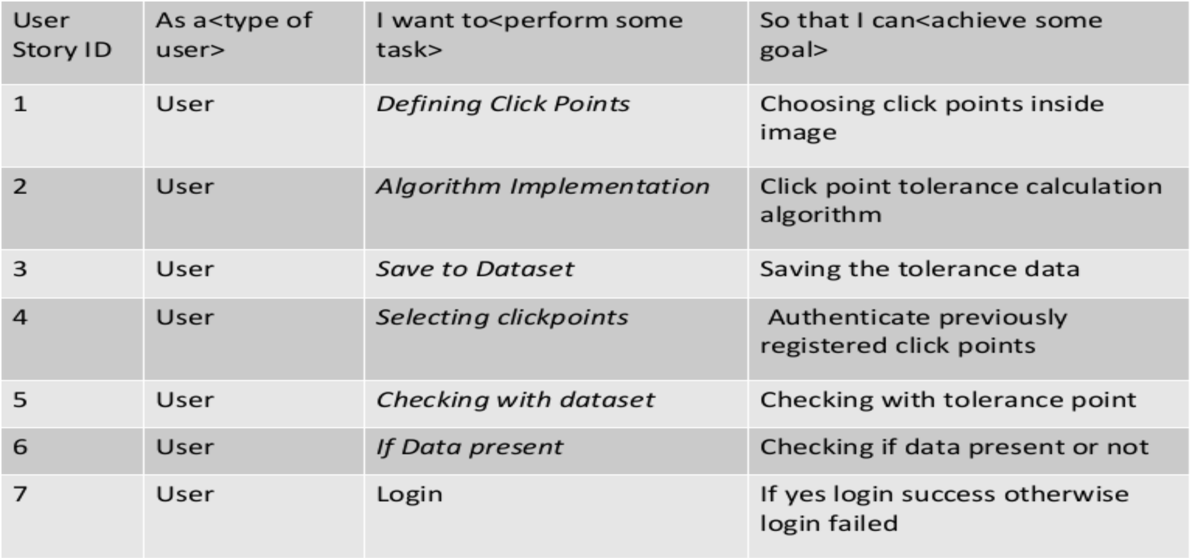
i)Selecting Click points
ii)Checking with Dataset

Sprint 3:Comparison and Result

i)if data present
ii)Login

3.4 User Story

A key component of agile software development is putting people first, and user-stories put actual end users at the center of the conversation. Stories use non-technical language to provide context for the development team and their efforts. After reading a user story, the team knows why they are building what they're building and what value it creates. A user story is a tool used in agile software development to capture a description of a software feature from an end user perspective. The user story describes the type of user, what they want and why. A user story helps to create a simplified description of a requirement. User stories are one of the core components of an agile program. They help provide a user-focused framework for daily work which drives collaboration, creativity, and a better product overall. The user story of system is,

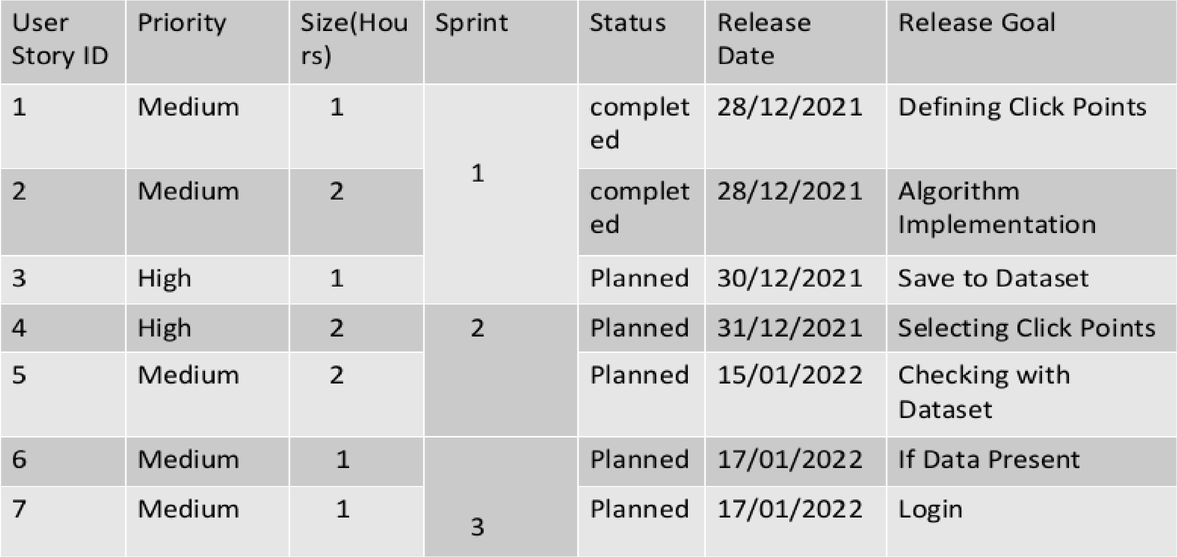


User Story ID	As a<type of user>	I want to<perform some task>	So that I can<achieve some goal>
1	User	*Defining Click Points*	Choosing click points inside image
2	User	*Algorithm Implementation*	Click point tolerance calculation algorithm
3	User	*Save to Dataset*	Saving the tolerance data
4	User	*Selecting clickpoints*	Authenticate previously registered click points
5	User	*Checking with dataset*	Checking with tolerance point
6	User	*If Data present*	Checking if data present or not
7	User	Login	If yes login success otherwise login failed

Figure 3.1: User Story

3.5 Product Backlog

A product backlog is a list of the new features, changes to existing features, bug fixes, infrastructure changes or other activities that a team may deliver in order to achieve a specific outcome.The product backlog is the single authoritative source for things that a team works on. That means that nothing gets done that isn't on the product backlog. Conversely, the presence of a product backlog item on a product backlog does not guarantee that it will be delivered. It represents an option the team has for delivering a specific outcome rather than a commitment.It should be cheap and fast to add a product backlog item to the product backlog, and it should be equally as easy to remove a product backlog item that does not result in direct progress to achieving the desired outcome or enable progress toward the outcome. The Scrum Product Backlog is simply a list of all things that needs to be done within the project. It replaces the traditional requirements specification artifacts. These items can have a technical nature or can be user-centric e.g. in the form of user stories.The product backlog of the system is given below figure.

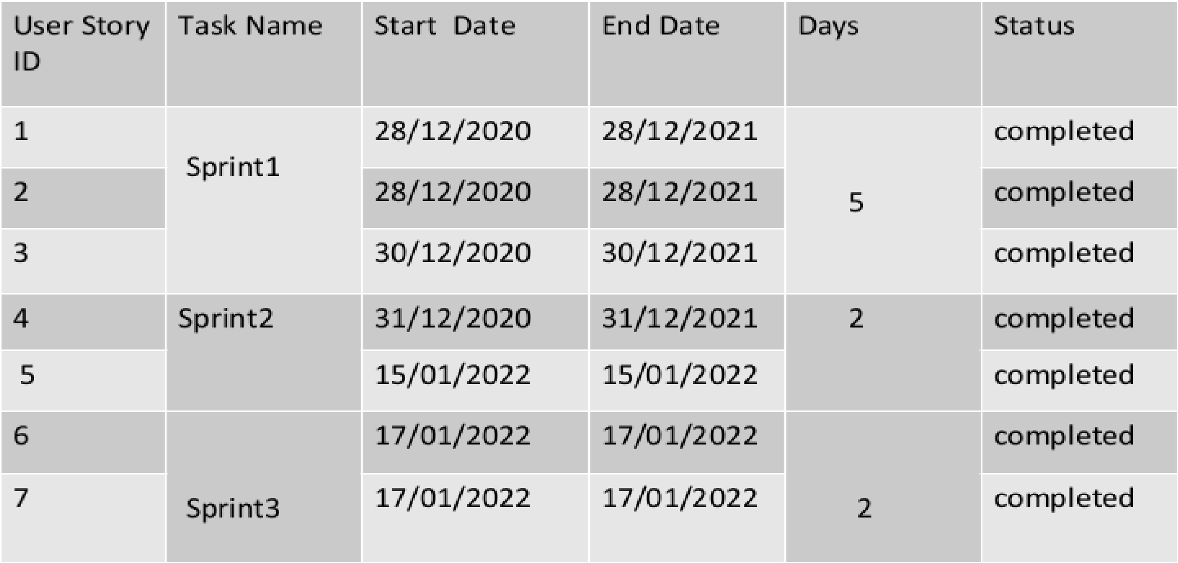


User Story ID	Priority	Size(Hours)	Sprint	Status	Release Date	Release Goal
1	Medium	1	1	completed	28/12/2021	Defining Click Points
2	Medium	2		completed	28/12/2021	Algorithm Implementation
3	High	1		Planned	30/12/2021	Save to Dataset
4	High	2	2	Planned	31/12/2021	Selecting Click Points
5	Medium	2		Planned	15/01/2022	Checking with Dataset
6	Medium	1	3	Planned	17/01/2022	If Data Present
7	Medium	1		Planned	17/01/2022	Login

Figure 3.2: Product Backlog

3.6 Project Plan

A project plan that has a series of tasks laid out for the entire project, listing task duration,responsibility assignments, and dependencies. Plans are developed in this manner based on the assumption that the Project Manager, hopefully along with the team, can predict up front everything that will need to happen in the project, how long it will take, and who will be able to do it. Project plan is given below figure. The project has Three sprints,

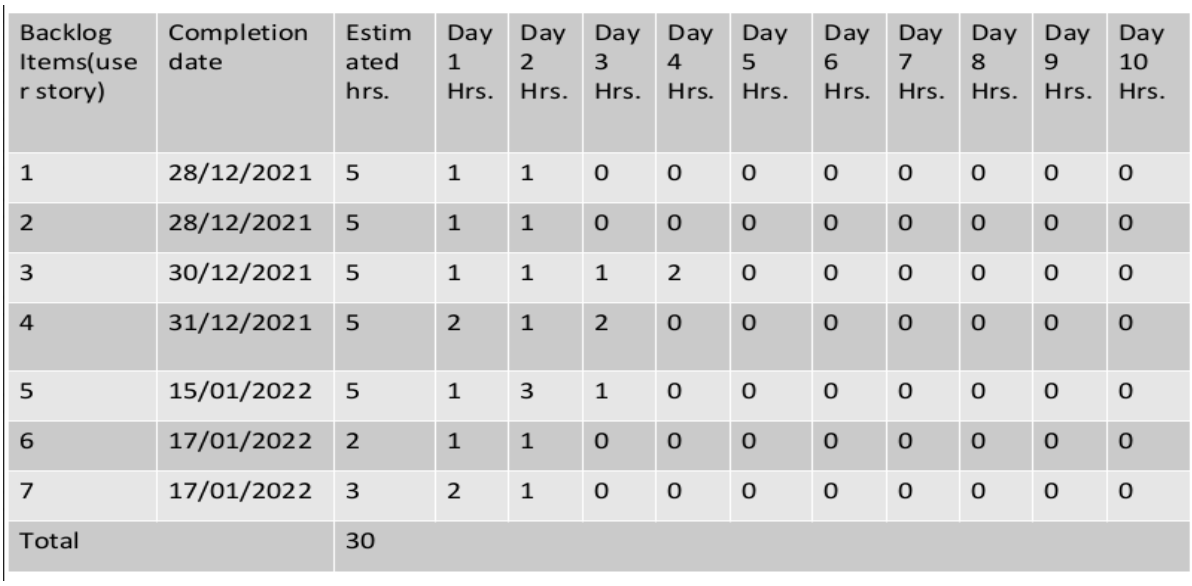


User Story ID	Task Name	Start Date	End Date	Days	Status
1	Sprint1	28/12/2020	28/12/2021	5	completed
2		28/12/2020	28/12/2021		completed
3		30/12/2020	30/12/2021		completed
4	Sprint2	31/12/2020	31/12/2021	2	completed
5		15/01/2022	15/01/2022		completed
6	Sprint3	17/01/2022	17/01/2022	2	completed
7		17/01/2022	17/01/2022		completed

Figure 3.3: Project Plan

3.7 Sprint Plan

The sprint plan is a list of tasks identified by the Scrum team to be completed during the Scrum sprint. During the sprint planning meeting, the team selects some number of product backlog items, usually in the form of user stories, and identifies the tasks necessary to complete each user story. Most teams also estimate how many hours each task will take someone on the team to complete.

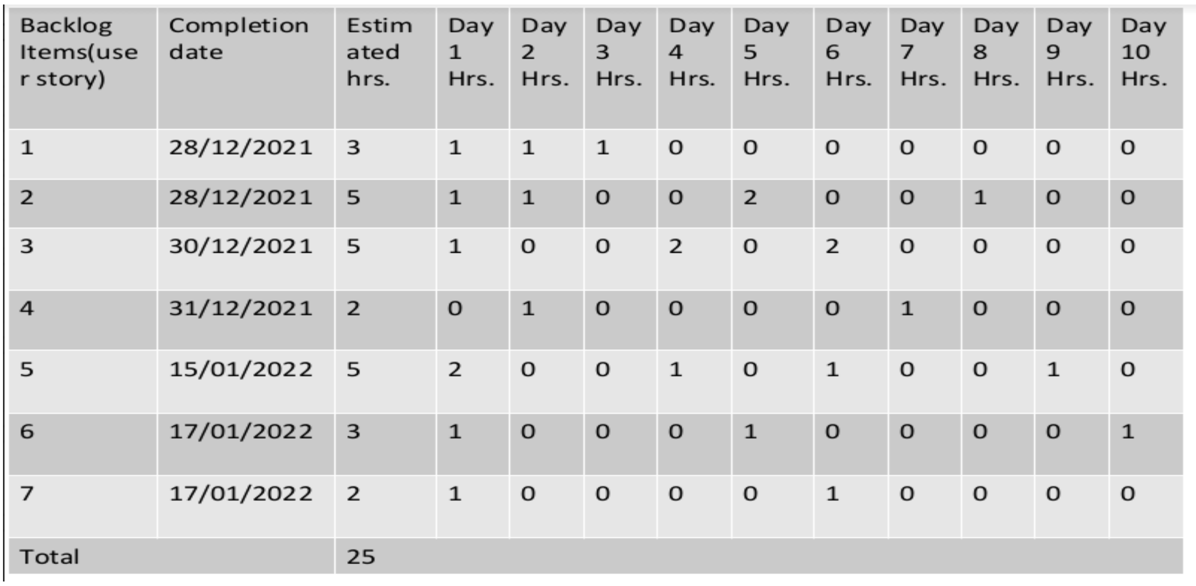


Backlog Items(user story)	Completion date	Estimated hrs.	Day 1 Hrs.	Day 2 Hrs.	Day 3 Hrs.	Day 4 Hrs.	Day 5 Hrs.	Day 6 Hrs.	Day 7 Hrs.	Day 8 Hrs.	Day 9 Hrs.	Day 10 Hrs.
1	28/12/2021	5	1	1	0	0	0	0	0	0	0	0
2	28/12/2021	5	1	1	0	0	0	0	0	0	0	0
3	30/12/2021	5	1	1	1	2	0	0	0	0	0	0
4	31/12/2021	5	2	1	2	0	0	0	0	0	0	0
5	15/01/2022	5	1	3	1	0	0	0	0	0	0	0
6	17/01/2022	2	1	1	0	0	0	0	0	0	0	0
7	17/01/2022	3	2	1	0	0	0	0	0	0	0	0
Total		30										

Figure 3.4: Sprint Plan

3.8 Sprint Actual

Actual sprint backlog is what adequate sprint planning is actually done by project team there may or may not be difference in planned sprint backlog. The detailed sprint backlog (Actual) is given below.



Backlog Items(user story)	Completion date	Estimated hrs.	Day 1 Hrs.	Day 2 Hrs.	Day 3 Hrs.	Day 4 Hrs.	Day 5 Hrs.	Day 6 Hrs.	Day 7 Hrs.	Day 8 Hrs.	Day 9 Hrs.	Day 10 Hrs.
1	28/12/2021	3	1	1	1	0	0	0	0	0	0	0
2	28/12/2021	5	1	1	0	0	2	0	0	1	0	0
3	30/12/2021	5	1	0	0	2	0	2	0	0	0	0
4	31/12/2021	2	0	1	0	0	0	0	1	0	0	0
5	15/01/2022	5	2	0	0	1	0	1	0	0	1	0
6	17/01/2022	3	1	0	0	0	1	0	0	0	0	1
7	17/01/2022	2	1	0	0	0	0	1	0	0	0	0
Total		25										

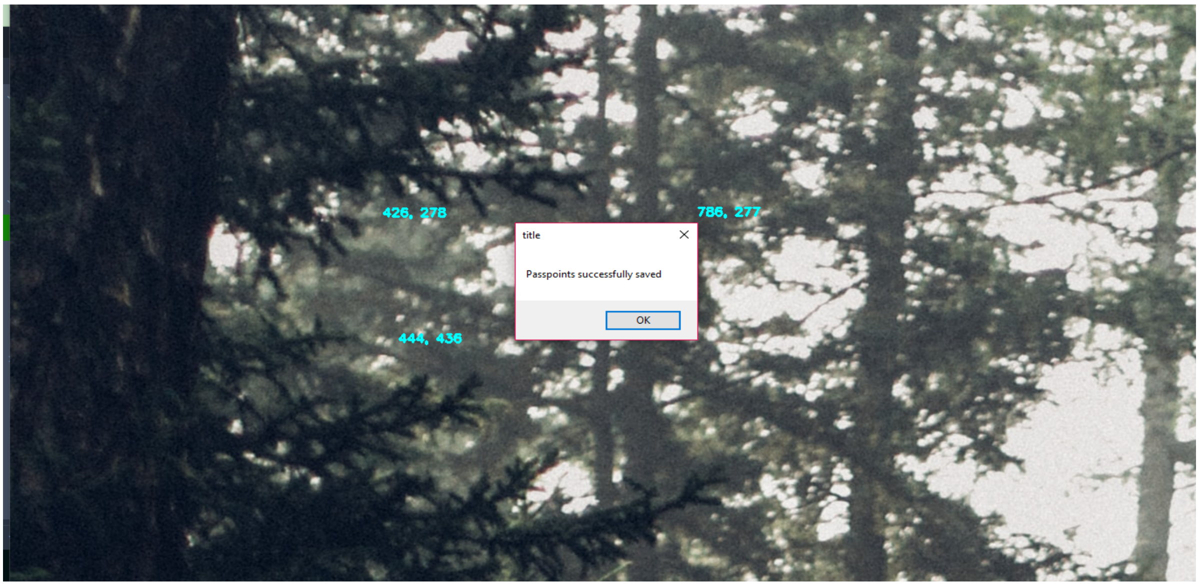
Figure 3.5: Sprint Actual

Chapter 4

Results and Discussions

4.1 Results

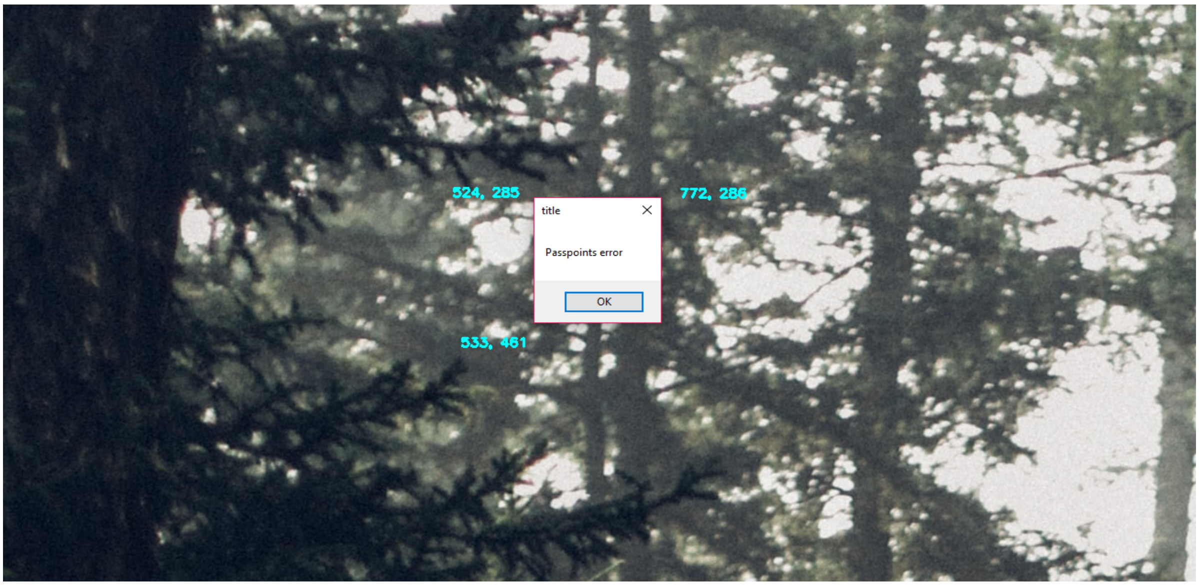
Password Registration:



Passpoints successfully saved

Figure 4.1: Registration

Password Authentication:



Passpoints error

Figure 4.2: Authentication

Chapter 5

Conclusions

Usually people use passwords that can be easily guessed, so that it does not becomes hard to remember. Hence to encounter this problem, researches have developed graphical password authentication methods that use pictures as passwords. Graphical passwords are an alternative to text-based passwords where user is asked to recall an image or parts of an image instead of a word. We are further discussing new and more secure graphical password system called pass points. In pass points system users can create many points click sequence on a background image. The graphical password is new technique which is more secure than text-based passwords. In graphical passwords, sequence of clicks is generated to derive the password. The click events are performed on same image.

In this project,we take an image as password instead of text password.there are two parts in this project:registration and main.At registration,we have to do atleast four click on an image for creating a password.At the fourth click a message box appear ”passpoint saved” successfully”.Next is main part ,in which we have to click four points ,and at fourth click a message box will appear ”passpoint saved” if the point matches to the points that we click at registration time ,or ”passpoint error” if it not match.

The system is more applicable in Digital wallets and Crypto currency because it is hard method.The only disadvantage is if users forget the password, it cannot retrieve it.

5.1 Future Enhancement

In future it has great scope. It can be used everywhere instead of text-based password . We can increase the security of this system by increasing the number of levels used, the number of tolerance squares used. Presently there are many authentication system but they have their own advantages and disadvantages.

This system is more secure and cheap than old methodologies. As well as this system allows more reliable and easily recognizable system to the users. As how we have written over this system can be best alternative to the text password.

References

[1] https://shsuir.tdl.org/shsuir/bitstream/handle/20.500.11875/1164/0781.pdf?sequence=1.

[2] https://ieeeplore.ieee.org/document/6208293/.

[3] https://ieeexplore.ieee.org/document/4679917/

Appendix

Source Code

```
Registration.py

import cv2
import numpy as np
import csv
import win32api
#This will display all the available mouse click events
#events = [i for i in dir(cv2) if ’EVENT’ in i]
#print(events)
#This variable we use to store the pixel location
refPt = []
global a
a=0
with open(’points.csv’, ’w’, newline=’’) as file:
  writer = csv.writer(file)
  writer.writerow(["SN", "x", "y"])
#click event function
def click_event(event, x, y, flags, param):
   if event == cv2.EVENT_LBUTTONDOWN:
      global a
      print(a)
      if(a<4):
          print(x,",",y)
          l=x-20
          r=x+20
          while l<r:
            t=y+20
            b=y-20
            while b<t:
               print(l,",",b)
               with open(’points.csv’, ’a’, newline=’’) as file:
                 writer = csv.writer(file)
                 writer.writerow([a, l, b])
               b=b+1
            l=l+1
          a=a+1
         if(a==4):
            win32api.MessageBox(0, ’Passpoints successfully saved ’, ’title’)
            cv2.destroyAllWindows()
      refPt.append([x,y])
      font = cv2.FONT_HERSHEY_SIMPLEX
      strXY = str(x)+", "+str(y)
      cv2.putText(img, strXY, (x,y), font, 0.5, (255,255,0), 2)
      cv2.imshow("image", img)
```

Appendix

```
#Here, you need to change the image name and it’s path according to your directory
img = cv2.imread("image.jpg")
cv2.imshow("image", img)
#calling the mouse click event
cv2.setMouseCallback("image", click_event)
cv2.waitKey(0)
cv2.destroyAllWindows()
```

Main.py

```
import cv2
import numpy as np
import csv
import win32api
flag=0
login = False
refPt = []
global a
a=0
#click event function
def click_event(event, x, y, flags, param):
   if event == cv2.EVENT_LBUTTONDOWN:
      global a
      print(a)
       if(a<4):
          print(x,",",y)
         with open(’points.csv’, ’r’) as csvfile:
            csv_reader = csv.reader(csvfile)
            for row in csv_reader:
               if row[0]== a and row[1] == x and row[2] == y:
                  login = True
               else:
                  login = False
                  flag=1
          a=a+1
         if(a==4):
            if(flag==0):
               win32api.MessageBox(0, ’Passpoints successfull ’, ’title’)
            else:
               win32api.MessageBox(0, ’Passpoints error ’, ’title’)
            cv2.destroyAllWindows()
       refPt.append([x,y])
      font = cv2.FONT_HERSHEY_SIMPLEX
      strXY = str(x)+", "+str(y)
      cv2.putText(img, strXY, (x,y), font, 0.5, (255,255,0), 2)
      cv2.imshow("image", img)
#Here, you need to change the image name and it’s path according to your directory
img = cv2.imread("image.jpg")
cv2.imshow("image", img)
#calling the mouse click event
cv2.setMouseCallback("image", click_event)
cv2.waitKey(0)
cv2.destroyAllWindows()
```